

(٢) من مبرهنات بيان x, y, z ثلاثي جيبًا عكسًا، وهي:

$$d(r, s) = 1$$

$$x = r^2 - s^2 \quad y = 2rs \quad z = r^2 + s^2$$

و r, s عددين زوجيين أو فرديين

(٣) إذا كان $3 \mid y$ يتم المطلوب

(١) إذا كان $3 \nmid y$: $3 \nmid 2rs$ وبالنسبة لـ 3 ان يقسم r و s

$3 \nmid 2$ و $3 \nmid r$ و $3 \nmid s$ (لان r و s أوليان عدديًا يعنيهما)

معنى ذلك باقي r و s على 3 إما 1 أو 2

$$s = 3q_1 + 1 \quad \vee \quad r = 3q_1 + 1$$

$$s = 3q_1 + 2 \quad \vee \quad r = 3q_1 + 2$$

عندئذ

$$x = r^2 - s^2 = (3q_1 + 2)^2 - (3q_1 + 1)^2 \quad (٣')$$

وبالنسبة 3 يقسم x

$$x = r^2 - s^2 = (3q_1 + 1)^2 - (3q_1 + 2)^2 \quad (٣'')$$

وبالنسبة 3 يقسم x

(٤) مركز الدائرة القائمة في مثلث ΔABC هو نقطة تلاقي المتوسطات

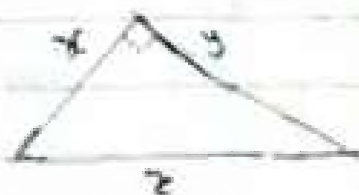
مركز الدائرة المارة بـ D من المثلث ΔABC نقطة تلاقي المتوسطات

المفرقة AD و BE ضلعين من المثلث ΔABC و BC الضلع

R نصف قطر الدائرة القائمة بأضلاع المثلث

وبالنسبة ضلعه المثلث

$$S = \frac{1}{2} xy = \frac{1}{2} R (x + y + z)$$



ولكن عاين (x, y, z) التي متساوية في (r, s) وبالنسبة لـ k مبرهنة

$$\begin{cases} x = r^2 - s^2 & \Rightarrow x = k(r^2 - s^2) \\ y = 2rs & \Rightarrow y = k(2rs) \\ z = r^2 + s^2 & \Rightarrow z = k(r^2 + s^2) \end{cases}$$

$$R = \frac{x \cdot y}{x + y + z} = \frac{k^2 \cdot 2 \cdot r \cdot s (r^2 - s^2) \rightarrow (r+s)(r-s)}{k(r^2 - s^2 + 2rs + r^2 + s^2)}$$

$$= \frac{(r+s)(r-s)}{k(r^2 - s^2 + 2rs + r^2 + s^2)} = k \cdot s(r-s)$$

وبالنسبة لـ R عدد صحيح (لأن k عدد صحيح و s عدد صحيح و $(r-s)$ عدد صحيح) وبالنسبة لـ k عدد صحيح

المطابقات

تعريف:

لنكون $a, b \in \mathbb{Z}$ ونسكن $m \in \mathbb{Z}^+$ نقول a و b مطابقان modulo m اذا كان
 لهما نفس الباقي عند تقسيمه على m اي اذا كان $m \mid (a-b)$
 ونكتب $a \equiv b \pmod{m}$

$$a \equiv b \pmod{m}$$

علا نقول a مطابق b بالمعاس m .

مجموعات البواقي:

نعلم ان عند تقسيم اي عدد n على m يمكن

$$n = q \cdot m + r, \quad 0 \leq r < m, \quad m > 1$$

$$r \in \{0, 1, 2, \dots, m-1\}$$

وبالتالي نعرف \mathbb{Z} الى مجموعة m رتبة و m باقي ممكن ان يكون

مجموعات البواقي m هذه المجموعات

المكونة من المجموعات تشكل \mathbb{Z}_m .

١- اتحادها هو \mathbb{Z} .

٢- تقاطع اي اثنين مختلفين \emptyset .

٣- اية عناصر لا يساوي \emptyset .

اي عدد n من \mathbb{Z} هو في

$$\mathbb{Z}_m = \{m \cdot t + r : t \in \mathbb{Z}\}$$

فكل اعداد n من \mathbb{Z} هي في \mathbb{Z}_m اي في \mathbb{Z}_m .

نكتب $m = 6$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

لها 6 عناصر

مجموعة \mathbb{Z}_6 هي مجموعة البواقي modulo 6

مجموعة \mathbb{Z}_6 هي مجموعة البواقي modulo 6

وبالتالي هذه المجموعة هي مجموعة البواقي modulo 6

وبالنسبة لـ $\{0, 1, 2, 3, 4, 5, 6\}$ مجموعة البواقي السالبة الصغرى والمفيدة

ملاحظة:

1- هذا تعريف للتطابق ينتج أنه إذا كان $a \equiv b \pmod{m}$ فإن a و b ينتميان إلى نفس البواقي بالتقسيم على m .
إذا كان $a \not\equiv b \pmod{m}$ فهما ينتميان إلى باقين مختلفين بالتقسيم على m .

2- أنه أي عدد صحيح n مطابق لـ r باقي قسمته على العدد m لأن $n = q \cdot m + r$

حيث r حقيقته الصغرى وبالنسبة

$$n - r = q \cdot m \quad (\Leftrightarrow)$$

$$m \mid (n - r) \quad \text{وبالنسبة}$$

$$n \equiv r \pmod{m}$$

الخواص العامة للتطابقات:

$$m \mid (a - b) \quad (\Leftrightarrow) \quad a \equiv b \pmod{m}$$

نفرق أن $a, b, c, d \in \mathbb{Z}$

1- العلاقة التطابق هي علاقة تكافؤ حقيقته الصغرى

$$\forall x \in \mathbb{Z} \quad x \equiv x \pmod{m}$$

الفكاسية

$$x \equiv y \pmod{m} \Rightarrow x \equiv y \pmod{m}$$

تناظرية

مفتية

$$x \equiv y \pmod{m} \wedge y \equiv z \pmod{m}$$

$$\Rightarrow x \equiv z \pmod{m}$$

$$ka \equiv kb \pmod{m}$$

$$\Leftrightarrow a \equiv b \pmod{m}$$

2- إذا كان

$$\forall k \in \mathbb{Z}$$

هوذا

$m \mid (a-b)$ يعني $a \equiv b \pmod{m}$
 اي $m \mid (a-b)$
 $m \mid (ka - kb)$
 $ka \equiv kb \pmod{m}$

3- اذا كان $a \equiv b \pmod{m}$ و $c \equiv d \pmod{m}$ وبشكل

$$a \pm c \equiv b \pm d \pmod{m}$$

ممكن في هذه الحالة وانما لا يتقرر ان $a \equiv b \pmod{m}$
 وكذلك

$$a \cdot c \equiv b \cdot d \pmod{m}$$

$$a^n \equiv b^n \pmod{m} \quad \text{و} \quad a \equiv b \pmod{m} \quad 4$$

حيث n عدد صحيح

ما سبق يتبين

$$f(x) = \sum_{i=0}^n c_i x^i \quad \text{اذا كان} \quad a \equiv b \pmod{m} \quad \text{و} \quad c_i \in \mathbb{Z} \quad \text{وبشكل} \quad (6)$$

(كثير الحدود) حيث

$$f(a) \equiv f(b) \pmod{m}$$

مثال

$$2 \equiv -4 \pmod{6}$$

$$\left\{ \begin{array}{l} 2 = 0 \cdot 6 + 2 \\ -4 = (-1) \cdot 6 + 2 \end{array} \right. \quad \text{حيث } a, b \text{ اعداد صحيحة}$$

$$6 \mid (2 - (-4)) = 2 + 4 = 6 \quad \text{او} \quad (6 \text{ يقسم فرقهما})$$

$$f(x) = x^2 - x + 10 \quad \text{وبشكل}$$

$$f(2) = 4 - 2 + 10 = 12$$

$$f(-4) = 16 + 4 + 10 = 30$$

$$12 \equiv 30 \pmod{6}$$

وہابی ہے

$$6 \mid (12-30) = -18$$

$$ka \equiv kb \pmod{m}$$

6 - اذکار

$$a \equiv b \pmod{m}$$

~ ip

$$d = d(m, k) \quad \text{ہے}$$

دلیل: لکھیں کہ k اور m کے لیے $d(m, k) = 1$ ہے

$$ka \equiv kb \pmod{m}$$

$$\Rightarrow a \equiv b \pmod{m}$$

ہم نے لکھا تھا کہ $a \equiv b \pmod{m}$ اور $a \equiv c \pmod{m}$ تو $b \equiv c \pmod{m}$ ہے۔

7 - اذکار $ka \equiv kb \pmod{p}$ ہے p اور k کے لیے $a \equiv b \pmod{p}$ ہے

$$a \equiv b \pmod{p}$$

8 - اذکار $a \equiv b \pmod{m}$ اور $n \mid m$ تو $a \equiv b \pmod{n}$ ہے

$$a \equiv b \pmod{n}$$

ہے

کیونکہ $n \mid (a-b)$ اور $n \mid m$ تو $n \mid (a-b)$ ہے

$$a \equiv b \pmod{n}$$

9 - اذکار $a, b \in \mathbb{Z}$ اور $m_i \in \mathbb{Z}^+$ اور $(m_1, m_2, \dots, m_k) = 1$ تو

$$a \equiv b \pmod{m_i}$$

ہے

$$a \equiv b \pmod{\ell\text{-cm}(m_1, m_2, \dots, m_k)}$$

10 - $a \equiv b \pmod{m}$ اور $m \in \ell\text{-cm}(m_1, m_2, \dots, m_k)$

چنان m_1, m_2, \dots, m_k نسبی m

ملاحظه: اذکان m_1, m_2, \dots, m_k اولیه نسبتاً همبسته باشند چنان

$$a \equiv b \pmod{(m_1, m_2, \dots, m_k)}$$

۱۰- اذکان $a \equiv b \pmod{p^r}$ صحت p عدد اول و $r \geq 1$ چنان

$$a^{p^s} \equiv b^{p^s} \pmod{p^{r+s}} \quad s \geq 0$$

بپهنای استقراری برسانیم
مثلاً:

$$a \equiv b \pmod{2^3} \Rightarrow a^{2^5} \equiv b^{2^5} \pmod{2^{3+5}}$$

استقراری $s \geq 0$ چنان $s=0$ $a^{p^0} \equiv b^{p^0} \pmod{p^{r+0}} \Rightarrow a \equiv b \pmod{p^r}$

العلاقه صحت چنان $s=0$

فرض کنیم چنان $s=k$ و نسبتاً چنان $s=k+1$

$$a^{p^k} \equiv b^{p^k} \pmod{p^{r+k}}$$

چنان یعنی $p^{r+k} \mid (a^{p^k} - b^{p^k}) \Rightarrow (a^{p^k} - b^{p^k}) = m_1 \cdot p^{r+k}, m_1 \in \mathbb{Z}$

$$a^{p^k} = m_1 \cdot p^{r+k} + b^{p^k}$$

فرض کنیم $a \equiv b \pmod{p}$

$$(a^{p^k})^p = (m_1 \cdot p^{r+k} + b^{p^k})^p$$

\downarrow
 $a^{p^{k+1}}$
 a

p توانی دوینوتن کن

بد آهمن، کد، لثاني $r+k+1$ ، $2r+2k+1$ --- وجميعا أكبر من $r+k+1$
 مجموع الحدود بد آهمن، کد، لثاني تقاطع، لثاني بالخاص

وهذا يعني أن a يطابق b في p^{k+1}

$$a \equiv b \pmod{p^{k+1}}$$

نريد: أثبت أن الفرق بين أي عددين n بالنظام العشري ومجموع أرقامه قبل الستة
 على 9.

أي يقبل عددا الستة على 9 إذا وفقط إذا قبل مجموع أرقامه الستة على 9.

إن أي عدد بالنظام العشري N يكتب على النحو

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 = (a_n, a_{n-1}, \dots, a_0)$$

وهذا يعني أن $10 \equiv 1 \pmod{9}$ وبالتالي

$$10^2 \equiv 1^2 \pmod{9}$$

$$(10)^k \equiv 1 \pmod{9} \text{ وتمام:}$$

$$N \equiv (a_n + a_{n-1} + \dots + a_1 + a_0) \pmod{9}$$

هذا يعني أن:

$$9 \mid (N - \sum_{i=1}^n a_i)$$

يقبل كد الستة على 9 إذا وفقط إذا قبل مجموع أرقامه الستة على 9

نريد: سؤال آخر

$$15 \mid (2^{4n} - 1)$$

أثبت أن هذا هل أي عددين صحيح موجب n يكون

أم (بين أن)

بیان آن: 2^n بقدر العشرة على 15 أم لا؟ لا يقبل العشرة لأن باقي عشرته على 15 لا يساوي 1

$$\frac{4^n}{2} = (2^4)^n$$

أي 2^4 يساوي 16 وهذا مطابق

$$2^4 \equiv 16 \equiv 1 \pmod{15}$$

$$(2^4)^n \equiv 1 \pmod{15}$$

$$\frac{4^n}{2} \equiv 1 \pmod{15} \Rightarrow 15 \mid (2^{4n} - 1)$$

بقي العشرة على 15 يساوي 1

مربعين - 3

أي $2^{2n} + 7$ يقبل العشرة على 8 أم لا

$$3^{2n} \equiv 1 \pmod{8}$$

نصف 7 أي طرفي المطابق

$$3^{2n} + 7 \equiv (7+1) \pmod{8}$$

وبالتالي

$$3^{2n} + 7 \equiv 0 \pmod{8}$$

وبالتالي

$$8 \mid (3^{2n} + 7)$$

أولاً: أليس في جميع مضروب K حقيقة العلاقة

$$31 \mid [(33)(26)^2 - K]$$

المضروب K مضروب عشرة
أي أولها باقي العشرة

$$(33)(26)^2 \equiv K \pmod{31}$$

نلاحظ

$$33 \equiv 2 \pmod{31}$$

$$26 \equiv -5 \pmod{31}$$

إذاً

$$Z_{31}$$

$$\overline{(26)} + \overline{(5)} = \overline{31} = \overline{0}$$

$$-(26) = 5$$

$$\overline{(26)} = -5$$

وبالتالي نظير 26 هو -5 يمكننا التعامل مع -5 بدلا من 26 الى

$$(26)^2 \equiv 25 \pmod{31}$$

$$(33)(26)^2 \equiv 50 \pmod{31}$$

$$\equiv 19 \pmod{31}$$

مباين $k=19$

عزيب

$$k! \text{ من } 1 \text{ الى } 1000$$

أو هذا حتى خمسة

$$\sum_{k=1}^{1000} k! = 1! + 2! + 3! + 4! + \dots$$

$$= 1 + 2 + 6 + 24 + 120 + \dots$$

ما في خمسة من 24 يادي الصفر

ما في خمسة من 24 يادي الصفر

بدؤا من الحجم الرابع من هذا المجموع جميع الحدود تقبل الصفة من 24 لفة تطابق من تطابق الصفر بالمقاس 24 وبالتالي

$$\sum_{k=1}^{1000} k! \equiv (1+2+6) \pmod{24}$$

أي تطابق و

$$k! \text{ من } 1 \text{ الى } 1000$$

أي ما في خمسة

عزيب

بين أن هناك عدد a يكون

$$a^2 \equiv 0 \text{ or } 1 \text{ or } 4 \pmod{8}$$

إذا كان a فردياً باقى مسخته على 8 م 1
 إذا كان a زوجي فانه على 4 م 0
 وبما $a^2 = 4q^2$ وبما $a = 2q$ وبما $a^2 = 4q^2$ وبما $a = 2q$
 وبما q كذا أن يكون زوجي أو فردي.

أو إذا كان لدينا عدداً باقى مسخته على 8 م 0 أو 1 أو 4
 وبما a^2 على 4 م 0 أو 1 أو 4
 وبما a^2 على 4 م 0 أو 1 أو 4

اختبارات قابلية القسمة:

عشرية:

① $(10)^n \equiv 0 \pmod{2^k}$

$$(10)^n \equiv 0 \pmod{2^k}$$

لكل عدد صحيح موجب k, n وكذلك

②

$$(10)^n \equiv 0 \pmod{5^k}$$

البرهان: ① و ②

$$10 = 2 \cdot 5 \text{ و } 10^k = 2^k \cdot 5^k$$

$$(10)^k = 2^k \cdot 5^k$$

نقط على كلتا التباديل

أي أن:

$$2^k \mid 10^k \quad \wedge \quad 5^k \mid 10^k$$

←

$$2^k \mid 10^n \quad \wedge \quad 5^k \mid 10^n \quad n > k$$

$$2^k \mid 10^n \quad \wedge \quad 5^k \mid 10^n \quad n > k$$

وبذلك يتم المطلوب.

مبرهنة: نعرف ان التمثيل العشري للعدد N هو الشكل،

$$N = (a_m a_{m-1} \dots a_1 a_0)_{10} \quad , \quad 0 \leq a_k \leq 10$$

a_k عدد صحيح.

ولنفرض

$$T = \sum_{k=0}^m (-1)^k a_k \quad \text{و} \quad S = \sum_{k=0}^m a_k$$

ولكن

$$N_k = (a_{k-1} \dots a_1 a_0)$$

عندئذ يكون:

$$\textcircled{1} \quad 2^k \mid N_k \quad \text{اذا وفقط اذا كان} \quad 2^k \mid N$$

$$N_1 = (a_0) \quad k=1 \quad \text{عربية واحدة}$$

يقبل البسطة عددا في 2 اذا وفقط اذا قبل آحاده البسطة في 2.

$$k=2$$

$$N_2 = (a_0, a_1) \quad 2^2 = 4$$

يقبل البسطة عددا في 4 اذا وفقط اذا قبل آحاده وعشرات في 4.

$$k=3$$

$$N_3 = (a_0, a_1, a_2) \quad 2^3 = 8$$

يقبل عددا البسطة في 8 اذا وفقط اذا قبل آحاده وعشرات ومئات البسطة في 8.

$$\textcircled{2} \quad 5^k \mid N_k \quad \text{اذا وفقط اذا كان} \quad 5^k \mid N$$

يقبل البسطة عددا في 5 اذا وفقط اذا كان آحاده، اياه او ك

$$\textcircled{3} \quad 3 \mid S \Leftrightarrow 3 \mid N$$

يقبل البسطة في 3 اذا وفقط اذا كان مجموع ارقامه يقبل البسطة في 3

$$\textcircled{4} \quad 9 \mid S \Leftrightarrow 9 \mid N$$

$$\textcircled{5} \quad 11 \mid T \Leftrightarrow 11 \mid N$$

مبرهنة:

$$n = (1000)q(n) + r(n) \quad \text{إذا كان}$$

فكان لعدد $C = 7 \cdot 11 \cdot 13$ فإنه

$$C \mid [q(n) - r(n)] \Leftrightarrow C \mid n$$

ملاحظة:

$$7 \cdot 11 \cdot 13 = 1001$$

$$q(n) - r(n) = q(n) - [n - 1000q(n)]$$
$$= 1001q(n) - n$$

وبالتالي 7 يقسم 1001 و 13 أيضاً و 11

$$q(n) - r(n) = 1001q(n) - n$$

جانب الشرط يلزم الكافي لكي يقسم أهمية عدد n يجب أن تقسم الطرف الآخر أي

$$q(n) - r(n)$$